

## PURPOSE

To establish the Michigan Department of Health and Human Services (MDHHS) policy for the use and sharing of protected health information or sensitive information with entities external to the department.

## DEFINITIONS

**Protected Health Information (PHI)** is information from a Health Insurance Portability and Accountability (HIPAA) covered component of MDHHS that can identify a person and contains health related data pertaining to that person.

**PII** is the acronym for Personally Identifiable Information. It is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

**Sensitive Information** is proprietary information that can identify an individual (Personally Identifiable Information or PII), protected by a federal or state confidentiality law other than HIPAA, or is provided to MDHHS by a federal, state, or other business partner on the condition that it be kept confidential.

## POLICY

It is the policy that use and sharing of MDHHS data externally will be documented in a signed written agreement known as a data use agreement. Data use agreements (DUA) can take many forms and formats, including data sharing agreements, non-disclosure agreements, contracts containing data sharing or data use provisions, and memoranda of understanding. Data use agreements outline what data will be shared, how data will be used, disclosed, and protected.

Data use agreements extending beyond a year must be reviewed annually.

This policy does not apply where MDHHS has determined a data use agreement is not necessary. While some determinations will be made on a case-by-case basis, areas generally exempt from this policy include, but are not limited to:

- Freedom of Information Act Requests (FOIA).

- Valid subpoenas or court orders.
- Where a contract or grant already covers the data sharing or work in question (such as, grant agreements, comprehensive agreements with local health departments, agreements with child placing agencies, etc.). Any requirements relating to data sharing should generally be added to the contract or grant instead of a separate DUA.
- Where law or policy authorizes disclosure without precondition, such as certain circumstances under the Child Protection Law (CPL), Mental Health Code (MHC), Public Health Code, Social Welfare Act or certain circumstances under other Department policy, such as BAM 310 or SRM 131.
- Where a program/business area has received a valid authorization or consent to share.
- Where an emergency exists requiring immediate sharing of the data with external partners to protect to the health and welfare of the public.

Questions and technical assistance about whether a data use agreement is necessary should be directed to the MDHHS compliance office at [MDHHS-ComplianceOffice@michigan.gov](mailto:MDHHS-ComplianceOffice@michigan.gov) or 517-284-1018. Legal questions can be directed to legal affairs.

## PROCEDURE

### REQUEST FOR DATA FROM EXTERNAL ENTITIES

- External entities may request MDHHS data for research, program evaluation, statistical analyses, public health, health care operations and other purposes.
- External entities interested in acquiring data from MDHHS may need to complete a MDHHS-5614, Data Request, form to initiate the data request process. Submit the completed MDHHS-5614 form to [MDHHS-DataRequests@michigan.gov](mailto:MDHHS-DataRequests@michigan.gov). A tracking number will be assigned to the data request.

**AGREEMENT  
DEVELOPMENT BY  
EXTERNAL ENTITIES**

- Entities external to MDHHS generally must complete the DCH-1294, Data Use and Non-Disclosure Agreement Concerning Protected Health Information or Other Confidential Information, form.

**Example:** University researchers, nonprofit agencies, federal agencies, policy institutes, tribes.

- State of Michigan agencies requesting MDHHS data may use the State of Michigan Data Sharing Agreement. State agencies may also use an Interagency Agreement (IA).

**Example:** Michigan State Police, DTMB, LARA.

- Federal agencies may use their own data sharing agreement form to submit for review and approval by the compliance office.

**Example:** Centers for Disease Control, Environmental Protection Agency.

- Tribes may use their own forms or memoranda of understanding to submit for review and approval by the compliance office.

**MDHHS  
Institutional  
Review Board**

Any request for data involving human subject research must be reviewed by the MDHHS Institutional Review Board (IRB). To reach the IRB, send an email to [MDHHS-IRB@michigan.gov](mailto:MDHHS-IRB@michigan.gov).

**MDHHS Sponsor**

Each MDHHS data source must have a MDHHS program sponsor when there is a request for data by an external entity. When there are two or more program sponsors due to multiple data sources, one of the sponsors will serve as the lead sponsor for the agreement.

The MDHHS sponsor is determined by the program leadership within the requested data program area. MDHHS sponsor's responsibilities include, but are not limited to:

- Assist in navigating the data use agreement through the process and is a point of contact between the data requestor and the compliance office.
- Conduct any necessary follow-up with the data requestor.
- Assist the data requestor with initiating the Institutional Review Board (IRB) review process.
- Serve as an initial point of contact for the data recipient to report any unauthorized use or disclosure of information.
- Request periodic updates and final reports of an evaluation or research project that would be of interest to the program area or MDHHS.
- Retain a copy of the executed data agreement to monitor for agreement compliance, data transfer/access termination dates, and evaluating for agreement renewal.

## **COMPLIANCE OFFICE REVIEW**

At a minimum the compliance office conducts a privacy review and a security review.

### **Security Review**

The security review evaluates the method for transferring data and the requestor's technical safeguards. The following list is the most common information that the security staff evaluates during the security review (not an exhaustive list):

- Type of data requested.
- Specific data security guidelines that apply to the data.
- The data requestor's entity and relationship to MDHHS.
- Transmission of the data.
- Who has access to the data such as subcontractors.
- Storage and safeguards utilized for the data.
- Has the requestor or subcontractor experienced a breach.
- Data disposal/destruction procedures.

## Privacy Review

The privacy review evaluates the substance and use of the requested data. The privacy review evaluates whether there is a legally permissible purpose for disclosure of the requested data. The following list is the most common information that the privacy and compliance staff evaluate during the privacy review (not an exhaustive list):

- Type of data requested, for example, what are the data elements, are they identified or de-identified, or a limited data set.
- The request purposes.
- The data source.
- Who is requesting the data and what is the relationship of the requestor to MDHHS.
- Whether data sharing is legally permissible/authorized and what is the legal basis to share, for example federal law, state law, MDHHS policy.
- The IRB's determination and whether there are consent forms to review.
- The risks/benefits/concerns in sharing this data.
- Whether the agreement is correct, complete and consistent with research proposal and the need for additional agreements.
- Whether access is appropriately limited.

Requests for protected health information from an MDHHS program covered by the Health Insurance Portability and Accountability Act (HIPAA) regulations may require that the parties enter a business associate agreement (BAA). Furthermore, a request for data that is subject to other federal, state, and/or local laws, rules, and/or regulations, such as the Family Education Rights and Privacy Act (FERPA), 42 CFR Part 2, Michigan Mental Health Code, or Michigan Public Health Code, may require additional terms to data use agreements at the discretion of the compliance office.

**AFTER  
COMPLIANCE  
OFFICE REVIEW**

If, after either the privacy or security review, it is determined that the DUA cannot be approved, the compliance office will notify the MDHHS sponsor of the reasons for the denial. The proposed data recipient will be notified by the MDHHS sponsor or the compliance office, as appropriate, after internal review of the determination.

**Agreement Execution**

MDHHS sponsor will be notified to obtain signatures on the agreement only after the compliance office review has been completed. Generally, the chief compliance officer should be the final signatory on the agreement. Change the order of signatures as circumstances warrant.

**Final Approval**

The chief compliance officer performs a final review of the data use agreement and if approved, signs it. Execute the data use agreement as of the date of the last signature.

**Agreement Distribution**

The compliance office will distribute the fully executed data use agreement to the MDHHS sponsor(s). The MDHHS sponsor is responsible for agreements distribution to the data requestor/recipient and makes note of any monitoring needs and milestones.

**Agreement Monitoring**

The MDHHS sponsor is responsible for monitoring compliance with terms of agreement and performing annual review. Review agreements extending beyond one year annually.

**AMENDMENTS TO  
AGREEMENTS**

**Extending the Agreement Term** - An agreement amendment form should be used when extending the term of the agreement by an additional year. Contact the compliance office for the form or for more information [at MDHHS-ComplianceOffice@michigan.gov](mailto:MDHHS-ComplianceOffice@michigan.gov).

**Substantive Amendments to Agreement** - Substantive amendments to a data use agreement (other than extension of the agreement's terms) will require the execution of a new data sharing agreement. Substantive amendments include, but are not limited to, changes in data source, adding or deleting data elements, changing data transmission methods, changing personnel identified for access, and modifying purpose. The data recipient, working with MDHHS data sponsor, will complete a new data use agreement and in a separate writing identify the amendments. Submit the new data agreement, along with the writing summarizing the amendments and the previously executed data use agreement, directly to the compliance office for review at [MDHHS-AgreementsReview@michigan.gov](mailto:MDHHS-AgreementsReview@michigan.gov).

#### **AGGREGATE OR SUMMARY STATISTICAL DATA REQUESTS**

Requests for aggregate or summary statistical data will follow this department policy and process. Administrations may develop and submit for review and approval by the compliance office their own procedures for logging and tracking data queries and requests for aggregate or summary statistical data.

#### **REFERENCES**

45 C.F.R. §164.501

45 C.F.R. §164.514(e)

APL 68D-110 Protected Health Information (PHI) Research Activities

APL 68D-050 Protected Health Information (PHI) Limited Data Set

#### **CONTACT**

For additional information concerning this policy and procedure, contact the MDHHS compliance office at [MDHHS-ComplianceOffice@michigan.gov](mailto:MDHHS-ComplianceOffice@michigan.gov) or 517-284-1018.